Chapter 1
System Log Messages Overview

The JUNOS software processes running on the router generate system log messages (also called syslog messages) to record events that occur on the router, including the following:

- Routine operations, such as creation of an Open Shortest Path First (OSPF) protocol adjacency or a user login into the configuration database
- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a child or peer process
- Emergency or critical conditions, such as router power-down due to excessive temperature

Each system log message identifies the software process that generated the message and briefly describes the operation or error that occurred. This manual provides more detailed information about each system log message and, when applicable, describes possible causes of the message and action you can take to correct error conditions.

> **Note**
>
> This version of the *JUNOS Internet Softw are System Log Messages* manual documents only some of the JUNOS system log messages. Future revisions of this manual, which generally will be released with new versions of the JUNOS Internet software, will likely include additional messages.

This chapter discusses the following topics:

System Logging Configuration Statements

To configure the router to log system messages, include the syslog statement at the [edit system] hierarchy level:

```
[edit system]
syslog {
    archive {
        files number;
        size size;
        (world-readable | no-world-readable);
    }
    console {
        facility level;
    }
    file filename {
        facility level;
        archive {
            files number;
            size size;
            (world-readable | no-world-readable);
        }
    }
    host hostname {
        facility level;
        facility-override facility;
        log-prefix string;
    }
    user (username | *) {
        facility level;
    }
}
```

Minimum System Logging Configuration

For the JUNOS software processes to generate system log messages, you must include the syslog statement at the [edit system] hierarchy level. Specify at least one destination for system log messages, as described in Table 2. For more information about the configuration statements, see “Configure System Logging” on page 5.

Table 2: Minimum Configuration Statements for System Logging

Destination	Minimum Configuration Statements

File	[edit system syslog]
	file *filename* {
	    facility level;
	}

Remote machine	[edit system syslog]
	host *hostname* {
	    facility level;
	}

Router console	[edit system syslog]
	console {
	    facility level;
	}

Terminal session of one, several. or all users	[edit system syslog]
	user (*username* | *) {
	    facility level;
	}

Configure System Logging

The JUNOS system logging utility is similar to the UNIX syslogd utility. When you configure system logging, you can direct messages to one or more destinations:

To a named file in a local file system, by configuring the file statement. See “Direct Messages to a Log File” on page 7.

To the terminal session of one or more specific users (or all users) when they are logged into the router, by configuring the user statement. See “Direct Messages to a User Terminal” on page 7.

To the router console, by configuring the console statement. See “Direct Messages to the Console” on page 8.

To a remote machine that is running the syslogd utility, by configuring the host statement. See “Direct Messages to a Remote Machine” on page 8.

Each message is assigned to a *facility*, which is a group of messages that are either generated by the same software process or concern a similar condition or activity (such as authentication attempts). To log the messages belonging to one or more facilities to a particular destination, specify each facility name as a separate statement within the set of statements for the destination. Table 3 lists the JUNOS system logging facilities.

Table 3: JUNOS System Logging Facilities

Facility	Type of Event or Error
any	Any (that is, includes messages from all facilities)
authorization	Authentication and authorization attempts
change-log	Changes to the JUNOS configuration
conflict-log	Configuration that is inconsistent with router hardware
daemon	Actions performed or errors encountered by various system daemons
firewall	Packet filtering actions performed by a firewall filter
ftp	Actions performed or errors encountered by the File Transfer Protocol (FTP) daemon
interactive-commands	Commands issued at the JUNOS command-line interface (CLI) prompt
kernel	Actions performed or errors encountered by the JUNOS kernel
pfe	Actions performed or errors encountered by the Packet Forwarding Engine
user	Actions performed or errors encountered by various user-space processes

Each message is assigned a *severity level*, which indicates how seriously it affects router functioning. When you configure logging for a facility and destination, you specify a severity level for each facility; messages from the facility that are rated at that level or higher are logged to the destination. Table 4 lists the severity levels in order from highest to lowest.

Table 4: System Log Message Severity Levels

Severity Level	Description
emergency	System panic or other condition that causes the router to stop functioning
alert	Conditions that require immediate correction, such as a corrupted system database
critical	Critical conditions, such as hard drive errors
error	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels
warning	Conditions that warrant monitoring
notice	Conditions that are not errors but might warrant special handling
info	Events or nonerror conditions of interest
debug	Software debugging messages; specify this level only when so directed by a technical support representative

To prevent log files from growing too large, the JUNOS system logging utility by default writes messages to a sequence of files of a defined size. You can configure the number of files, their maximum size, and who can read them. For more information, see “Configure Archiving of Log Files” on page 11.

When directing messages to a remote machine, you can configure features that make it easier to separate JUNOS-specific messages or messages generated on particular routers. For more information, see “Direct Messages to a Remote Machine” on page 8.

For a statement summary for the syslog statement, see the *JUNOS Internet Software Configuration Guide: Getting Started*.

For more information about configuring system logging, see the following sections:

Direct Messages to a Log File on page 7

Direct Messages to a User Terminal on page 7

Direct Messages to the Console on page 8

Direct Messages to a Remote Machine on page 8

Configure Archiving of Log Files on page 11

Examples: Configure System Logging on page 12

Direct Messages to a Log File

To direct system log messages to a file on the local disk of the router, include the file statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
file filename {
    facility level;
    archive {
        files number;
        size size;
        (world-readable | no-world-readable);
    }
}
```

The default directory for log files is /var/log; to specify a different directory on the local disk, include the complete pathname. For the list of logging facilities and severity levels, see Table 3 and Table 4 respectively.

You can also include the archive statement to configure the number, size, and permissions for a log file. For more information, see “Configure Archiving of Log Files” on page 11.

Direct Messages to a User Terminal

To direct system log messages to the terminal session of one or more specific users (or all users) when they are logged into the router, include the user statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
user (username | *) {
    facility level;
}
```

Specify one or more JUNOS usernames, separating multiple values with spaces, or use the asterisk (*) to indicate all users who are logged into the router. For the list of logging facilities and severity levels, see Table 3 and Table 4 respectively.

Direct Messages to the Console

To direct system log messages to the router console, include the console statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
console {
    facility level;
}
```

For the list of logging facilities and severity levels, see Table 3 and Table 4 respectively.

Direct Messages to a Remote Machine

To direct system log messages to a remote machine, include the host statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
host hostname {
    facility level;
    facility-override facility;
    log-prefix string;
}
```

Specify the remote machine's IP address or fully qualified hostname. The remote machine must be running either the standard syslogd utility or the JUNOS software, but we do not recommend directing messages to another router. For the list of logging facilities and severity levels, see Table 3 and Table 4 respectively.

You can also include the facility-override statement to assign an alternate facility and the log-prefix statement to prepend a prefix to system log messages, as described in the following sections:

Assign an Alternate Facility on page 8

Prepend a Prefix on page 11

Assign an Alternate Facility

Some of the facilities listed in Table 3 are specific to the JUNOS Internet software. When messages are written to a remote machine, they are assigned to a default remote facility that is available with the standard syslogd utility, because the remote machine might not be running JUNOS software. Table 5 lists the default remote facility for each local facility.

Table 5: Default Facilities for Messages Sent to a Remote Machine

Facility on Local Machine	Default Facility on Remote Machine
authorization	authorization
change-log	local6
conflict-log	local5
daemon	daemon
firewall	local3
ftp	ftp

Facility on Local Machine	Default Facility on Remote Machine
interactive-commands	local7
kernel	kernel
pfe	local4
user	user

The logging utility on the remote machine handles all messages in a facility in the same manner, regardless of whether the messages originate on another router or on the remote machine itself. For example, suppose you include the following statements on local-router to write messages from the authorization facility to a remote machine called monitor:

```
[edit system syslog]
host monitor {
    authorization info;
}
```

The default remote facility for the local authorization facility is also authorization. If the logging utility on monitor is configured to write messages belonging to the authorization facility to the file /var/log/auth-attempts, the file will contain both the messages generated when users log on to local-router and the messages generated when users log on to monitor. Although the name of the source machine appears in each system log message, the mixing of messages from multiple machines can make it more difficult to analyze the contents of the auth-attempts file.

To assign all messages sent to a remote machine to an alternate facility instead of to the default facilities listed in Table 5, include the facility-override statement at the [edit system syslog host *hostname*] hierarchy level:

```
[edit system syslog host hostname]
facility level;
facility-override facility;
```

Table 6 lists the facilities that you can specify in the facility-override statement.

In general, it makes sense to specify an alternate facility that is not already in use on the remote machine, such as one of the local*X* facilities. On the remote machine, you must also configure the logging utility to handle the messages assigned to the alternate facility in the desired manner.

Table 6: Facilities for the facility-override Statement

Facility	Description
authorization	Authentication and authorization attempts
daemon	Actions performed or errors encountered by various system daemons
ftp	Actions performed or errors encountered by the File Transfer Protocol (FTP) daemon
kernel	Actions performed or errors encountered by the JUNOS kernel
local0	Local facility number 0
local1	Local facility number 1
local2	Local facility number 2
local3	Local facility number 3
local4	Local facility number 4
local5	Local facility number 5
local6	Local facility number 6
local7	Local facility number 7
user	Actions performed or errors encountered by various user-space processes

Examples: Assign an Alternate Facility

Log all messages generated on the local router at the error level or higher to the local0 facility on the remote machine called monitor:

```
[edit system syslog]
host monitor {
    any error;
    facility-override local0;
}
```

Configure two routers located in California and two routers located in New York to send messages to a single remote machine called central-logger. The messages from California are aggregated into one facility (local1) and the messages from New York into another facility (local2).

Configure California routers to aggregate messages in the local1 facility:

```
[edit system syslog]
host central-logger {
    change-log info;
    facility-override local1;
}
```

Configure New York routers to aggregate messages in the local2 facility:

```
[edit system syslog]
host central-logger {
    change-log info;
    facility-override local2;
}
```

On central-logger, you could then configure the system logging utility to write messages from the local1 facility to /var/log/california-config and the messages from the local2 facility to /var/log/new-york-config.

Prepend a Prefix

To prepend a string to every system log message sent to a remote machine, include the log-prefix statement at the [edit system syslog host *hostname*] hierarchy level:

```
[edit system syslog host hostname]
facility level;
log-prefix string;
```

The prefix string can contain any alphanumeric character other than a space, the equal sign (=), or the colon (:). A colon and a space are appended to the string when the system log messages are written to the log.

Example: Pr epend a Pr efix

Prepend the string M40 to all messages to indicate that the router is an M40 router, and send the messages to the remote machine hardware-logger:

```
[edit system syslog]
host hardware-logger {
    any info;
    log-prefix M40;
}
```

When these configuration statements are included on a router called origin1, a message in the system logging file on hardware-logger looks like the following:

```
Mar 9 17:33:23 origin1 M40: mgd[477]: UI_CMDLINE_READ_LINE: user ‘root’, command ‘run
show version’
```

Configure Archiving of Log Files

By default, the JUNOS logging facility stops writing messages to a log file when the file reaches 128 KB in size. It closes the file and adds a numerical suffix, then opens and directs messages to a new file with the original name. By default, it creates up to 10 files before it begins overwriting the contents of the oldest file. The logging utility by default also limits the users who can read log files to the root user and users who have the JUNOS maintenance permission.

To configure different values that apply to all log files, include the archive statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
archive {
    files number;
    size size;
    (world-readable | no-world-readable);
}
```

To configure different values that apply to a particular log file, include the archive statement at the [edit system syslog file *filename*] hierarchy level:

```
[edit system syslog]
file filename {
    facility level;
    archive {
        files number;
        size size;
        (world-readable | no-world-readable);
    }
}
```

You can specify from 1 through 1000 files and a maximum size for each file of 64 KB (64k) through 1 GB (1g). To enable all users to read log files, include the world-readable statement. To restore the default permissions, include the no-world-readable statement.

Examples: Configure System Logging

Configure the handling of messages of various types, as described in the comments. Information is logged to two files, to a remote machine, to the terminal of user alex, and to the console:

```
[edit system]
syslog {
/* write all security-related messages to file /var/log/security */
    file security {
        authorization info;
        interactive-commands info;
    }
/* write messages about potential problems to file /var/log/messages: messages */
/* from “authorization” facility at level “notice” and above, messages from */
/* all other facilities at level “warning” and above */
    file messages {
        authorization notice;
        any warning;
    }
/* write all messages at level “critical” and above to terminal of user “alex” if she */
/* is logged in */
    user alex {
        any critical;
    }
/* write all messages from the “daemon” facility at level “info” and above, and messages */
/* from all other facilities at level “warning” and above, to the machine junipero.berry.net */
    host junipero.berry.net {
        daemon info;
        any warning;
    }
/* write all messages at level “error” or above to the system console */
    console {
        any error;
    }
}
```

Log messages about all CLI commands entered by users, and all authentication or authorization attempts, both to the file cli-commands and to the terminal of any user who is logged in:

```
[edit system]
syslog {
    file cli-commands {
        interactive-commands info;
        authorization info;
    }
    user * {
        interactive-commands info;
        authorization info;
    }
}
```

Configure the handling of messages generated when users issue JUNOS CLI commands, by specifying the interactive-commands facility at the following severity levels:

info—Logs a message when users issue any command at the CLI operational or configuration mode prompt. The example writes the messages to the file /var/log/user-actions.

notice—Logs a message when users issue the configuration mode commands rollback and commit. The example writes the messages to the terminal of user philip.

warning—Logs a message when users issue a command that restarts a software process. The example writes the messages to the console.

```
[edit system]
syslog {
    file user-actions {
        interactive-commands info;
    }
    user philip {
        interactive-commands notice;
    }
    console {
        interactive-commands warning;
    }
}
```

Log all changes in the state of alarms to the file /var/log/alarms:

```
[edit system]
syslog {
    file alarms {
        kernel warning;
    }
}
```

Display System Log Messages

To display system log messages, enter JUNOS CLI operational mode and issue either of the following commands:

```
user@host> show log log-filename
user@host> file show log-file-pathname
```

For more information about the commands, see the *JUNOS Internet Software Operational Mode Command Reference: Protocols, Class of Service, Chassis, and Management*.

System log messages have the following syntax:

```
timestamp [router-name] software-process[process-ID]: message-code: message-text
```

Table 7 describes the fields in each message.

Table 7: Fields in System Log Messages

System Log Message Field	Description
timestamp	Time at which the message was logged.
[*router-name*]	Router name.
software-process[*process-ID*]*:*	Name and process identifier (PID) of the JUNOS software process that generated the message.
message-code:	Code that identifies the type of message. The name begins with a prefix that identifies the generating software process or library. The entries in this manual are ordered alphabetically by this prefix. Table 8 lists and describes the software processes that generate the messages described in this manual.
message-text	Text of the system log message.

Examples: Display System Log Messages

Display the contents of the system log file /var/log/messages. (The /var/log directory is the default location for log files, so you do not need to include it in the filename. The messages filename is a commonly configured filename.)

```
# cli
user@host> show log messages
Apr 11 06:27:25 [host] mgd.last[1657]: UI_SCHEMA_MISMATCH_MINOR: Schema minor version
mismatch for package 6 (7. vs. 8)
Apr 11 06:27:25 [host] mgd.last[1657]: UI_DBASE_MISMATCH_SEQUENCE: Database header
sequence numbers mismatch for file '/var/db/juniper.db'
Apr 11 06:28:00 [host] mgd[629]: UI_CHILD_WAITPID: waitpid failed: pid 637, rc -1, status ffffffff:
No child processes
Apr 11 13:12:59 [host] mib2d[359]: SNMP_TRAP_LINK_DOWN: ifIndex 33, ifAdminStatus up(1),
ifOperStatus down(2), ifName at-3/1/0
```

Display the contents of the file /var/log/snmp-traps. With this command, specify the full pathname of the file:

```
# cli
user@host> file show /var/log/snmp-traps
Apr 10 19:23:41 [host] mib2d[359]: SNMP_TRAP_LINK_DOWN: ifIndex 33, ifAdminStatus up(1),
ifOperStatus down(2), ifName at-3/1/0
Apr 10 19:23:41 [host] mib2d[359]: SNMP_TRAP_LINK_DOWN: ifIndex 25, ifAdminStatus up(1),
ifOperStatus down(2), ifName at-3/1/0.0
Apr 10 19:23:41 [host] mib2d[359]: SNMP_TRAP_LINK_DOWN: ifIndex 21, ifAdminStatus up(1),
ifOperStatus down(2), ifName at-3/2/0
```

System Log Message Code Prefixes

System log message names begin with a prefix that indicates which JUNOS software process or subroutine library generated the message. Table 8 lists the prefixes for the messages described in this manual, briefly describes the source process or library, and refers you to the chapter that describes the messages with that prefix.

Table 8: Prefixes for System Log Message Codes

Message Code Prefix	Generating Process or Library
ACCT_	Accounting statistics process, which collects and records interface, filter, and class usage statistics. See “ACCT System Log Messages” on page 21.
BOOTPD_	Boot parameter process (tnp.bootpd), which provides the appropriate boot string to hardware components as they initialize. See “BOOTPD System Log Messages” on page 25.
CHASSISD_	Chassis process (chassisd), which controls the hardware components in the router. See “CHASSISD System Log Messages” on page 31.
DCD_	Interface process (dcd), which controls the physical interface devices and logical interfaces in the router. See “DCD System Log Messages” on page 45.
FSAD_	File System Access process (fsad), which which obtains boot-time information used by J20 gateway GPRS support node control-plane and user-plane (GGSN-C and GGSN-U) Physical Interface Cards (PICs) as they initialize. See “FSAD System Log Messages” on page 49.
GGSN_	Services PICs process (serviced), which provides the user interface for management and configuration of gateway GPRS support node control (GGSN-C) PICs. See “GGSN System Log Messages” on page 57.
JADE_	JUNOScript authentication process (jade), which authenticates and checks authorization of client applications using the JUNOScript API. See “JADE System Log Messages” on page 59.
LIBJNX_	The libjuniper library, which includes routines for creating and managing child processes, parsing machine and interface addresses, tracing, file I/O, and other functions. See “LIBJNX System Log Messages” on page 61.
LIBSERVICED_	Services PICs process (serviced, previously described for GGSN_ messages). See “LIBSERVICED System Log Messages” on page 65.
MIB2D_	Management Information Base II (MIB II) process (mib2d), which services requests for information gathered and reported by the Simple Network Management Protocol (SNMP). See “MIB2D System Log Messages” on page 67.
NASD_	Network Access Server process (nasd), which authenticates peers at the interface level. See “NASD System Log Messages” on page 73.
PWC_	Process Watch Controller process (pwc), which monitors GGSN-C processes for failures. See “PWC System Log Messages” on page 85.
RMOPD_	Remote SNMP operations process (rmopd), which services SNMP requests for execution of ping and traceroute operations. See “RMOPD System Log Messages” on page 95.
RPD_	Routing protocol process (rpd), which controls the routing protocols that run on the router. See “RPD System Log Messages” on page 101.
SERVICED_	Services PICs process (serviced, previously described for GGSN_ messages). See “SERVICED System Log Messages” on page 125.
SNMPD_	SNMP agent process (snmpd), which responds to SNMP requests. As necessary, it passes the requests to subagent processes running on its machine and forwards the traps they generate to the SNMP manager. See “SNMPD System Log Messages” on page 135.

Message Code Prefix	Generating Process or Library
SNMP_	Any JUNOS process that performs SNMP operations or is instrumented to generate a system log message when it sends an SNMP trap. See “SNMP System Log Messages” on page 153.
TFTPD_	Trivial File Transfer Protocol (TFTP) process (tnp.tftpd), which services requests from hardware components for the configuration files they use during initialization. See “TFTPD System Log Messages” on page 159.
UI_	Command-line interface (CLI) and management process (mgd), which together form the JUNOS user interface that accepts and processes input from users and client applications. See “UI System Log Messages” on page 165.

Display System Log Message Descriptions

This manual lists the messages available at the time of its publication. To display the most current list of messages, enter JUNOS CLI operational mode and issue the following command:

```
user@host> help syslog ?
```

To display the complete description of a particular message, substitute its name for the variable *code*:

```
user@host> help syslog code
```

For a description of the fields in a system log message description, see “Interpret System Log Message Descriptions” on page 18.

Examples: Display System Log Message Descriptions

Display the list of all currently available system log message descriptions:

```
user@host> help syslog ?
Possible completions:
  <syslog-tag>            Syslog tag
  BOOTPD_ARG_ERR          Command-line option was invalid
  BOOTPD_BAD_ID           Request failed because assembly ID was unknown
  BOOTPD_BOOTSTRING       tnp.bootpd provided boot string
  BOOTPD_CONFIG_ERR       tnp.bootpd could not parse configuration file; used default settings
  BOOTPD_CONF_OPEN        tnp.bootpd could not open configuration file
  BOOTPD_DUP_REV          Extra boot string definitions for revision were ignored
---(more 2%)---
```

Display the description of the UI_CMDLINE_READ_LINE message:

```
user@host> help syslog UI_CMDLINE_READ_LINE
Name:        UI_CMDLINE_READ_LINE
Message:     User '<user>', command '<input>'
Help:        User entered command at CLI prompt
Description: The indicated user typed the indicated command at the CLI prompt and pressed the
             Enter key, sending the command string to the management process (mgd).
Type:        Event: This message reports an event, not an error
Severity:    info
```

Interpret System Log Message Descriptions

This manual uses a reference page format to describe system log messages. Table 9 describes the sections in a reference entry.

Table 9: System Log Message Fields

Field	Description
System Log Message	Text of the message displayed on the console and placed in the log file. The first line is the message code in all capital letters. The prefix on each code identifies the JUNOS software process or library that generated the message and the rest of the code indicates the specific event or error. Table 8 lists the prefixes for which this manual includes reference entries. The second line in this field is a brief description generated by the JUNOS software process or library. When the message is written to a system log, a specific value is substituted for each variable name that appears in italics in the reference entries.
Description	More detailed explanation of the message.
Type	Category to which the message belongs: Error: The message reports an error or failure condition that might require corrective action. Event: The message reports a condition or occurrence that is considered a normal operation not requiring corrective action.
Severity	Message severity level as described in Table 4.
Cause	(Optional) Possible cause of the operation that generated the system log message. There can be more than one cause.
Action	(Optional) Action to perform to resolve the error or failure condition described in the message. If this field does not appear in an entry, either no action is required or the action is self-explanatory.